資料２－１

フィッシングSMS対策の現状取組みについて

NTT docomo

2024年 3月 14日

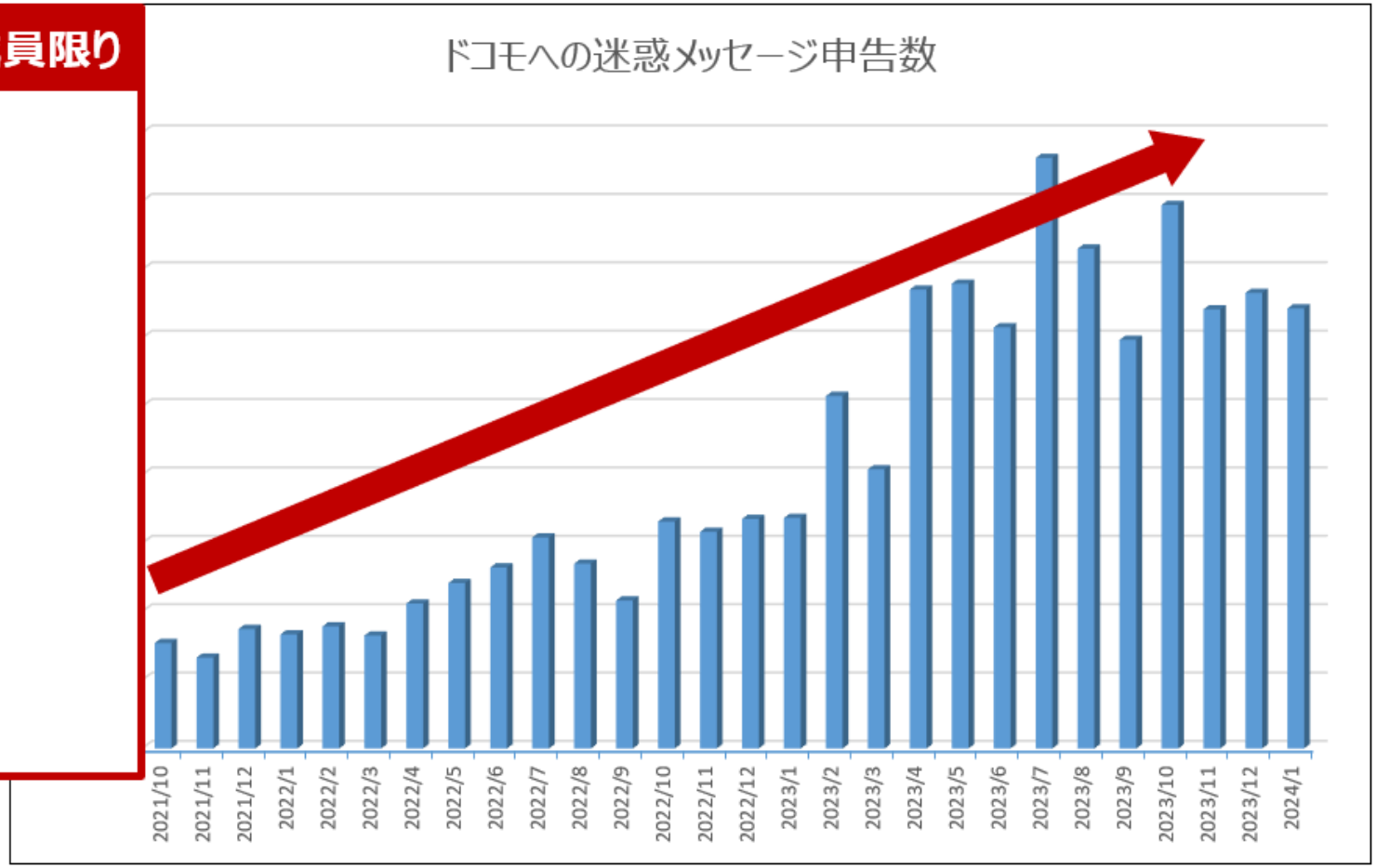
本日のご説明の流れ

- フィッシングSMS対策機能の提供
- お客様への注意喚起・周知啓発の取組み
- 携帯電話事業者・関係機関との情報連携
- マルウェア感染によるSMS大量送信被害への特別対応
- まとめ

フィッシングSMS等に関するお客様申告状況

- ドコモへの迷惑メッセージ申告数は、2020年以降も増加傾向が続いている状況
- 危険SMS拒否設定等の対策を実施しているものの、迷惑メッセージの多様化・巧妙化が激しく申告数が増加している状況

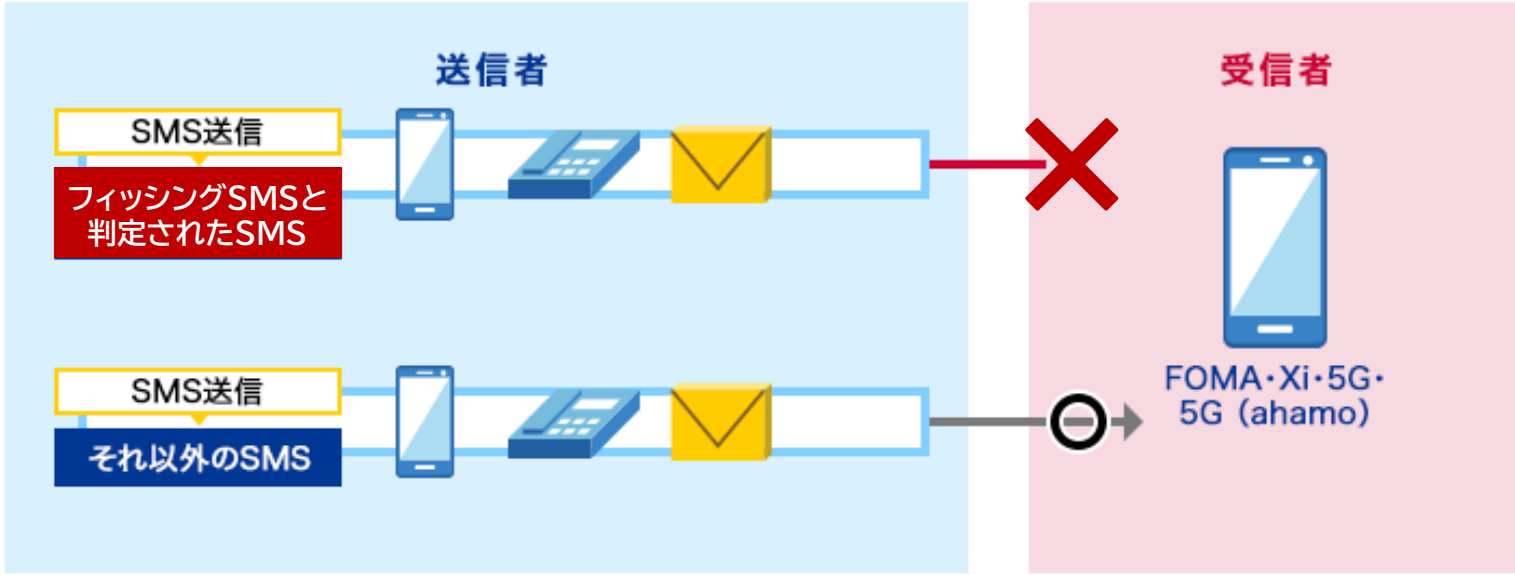
構成員限り



フィッシングSMS対策機能の提供

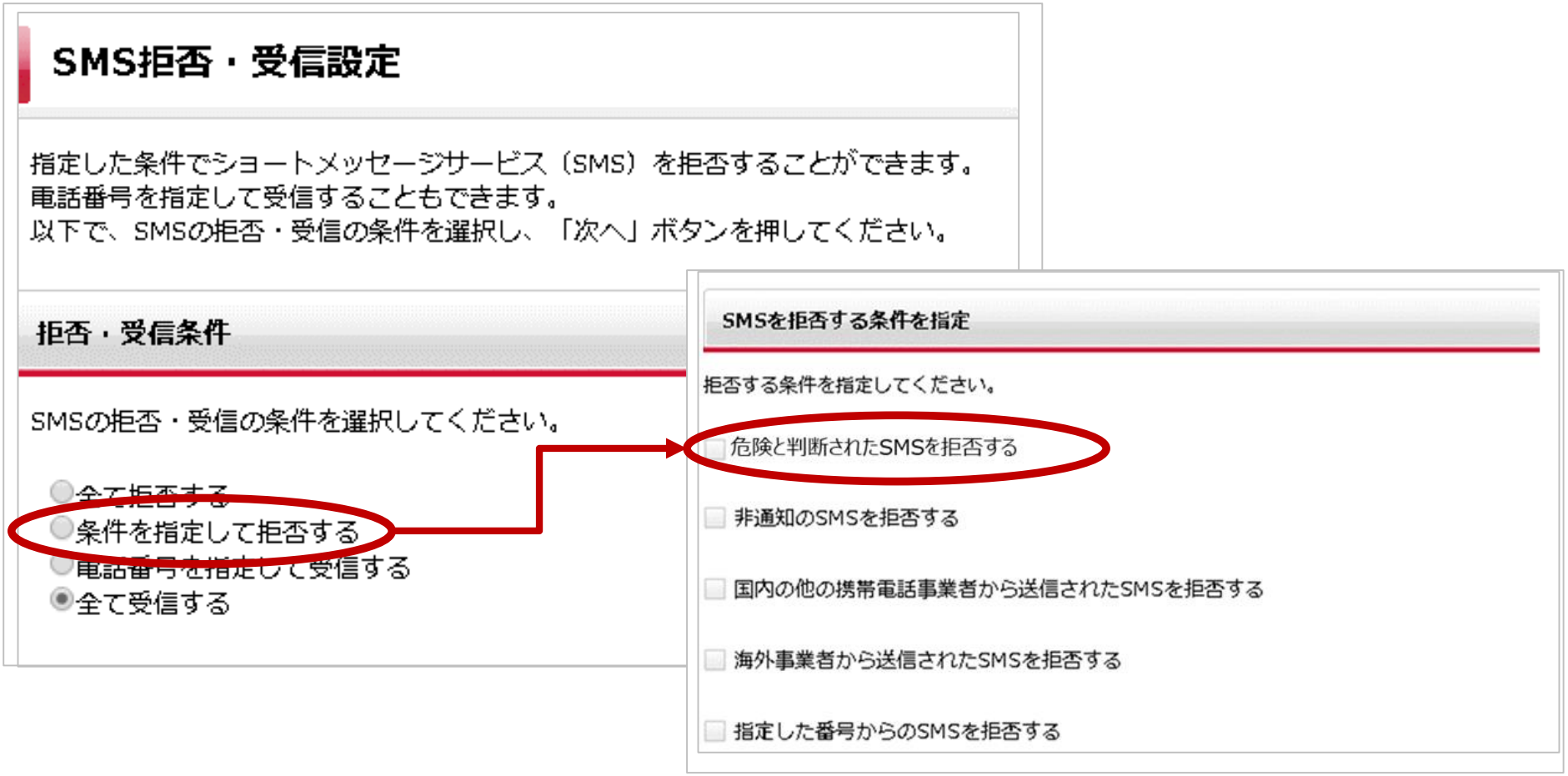
「危険SMS拒否設定」の提供

- SMSフィッシング詐欺対策として、2022年3月に「危険SMS拒否設定」を提供開始
- 危険サイトのURLや電話番号が含まれる等、フィッシングSMSと判定したSMSの受信をブロック
- 危険SMS拒否設定は申込み不要で提供(拒否設定を希望しない場合はオプトアウトにて設定)



「危険SMS拒否設定」の提供

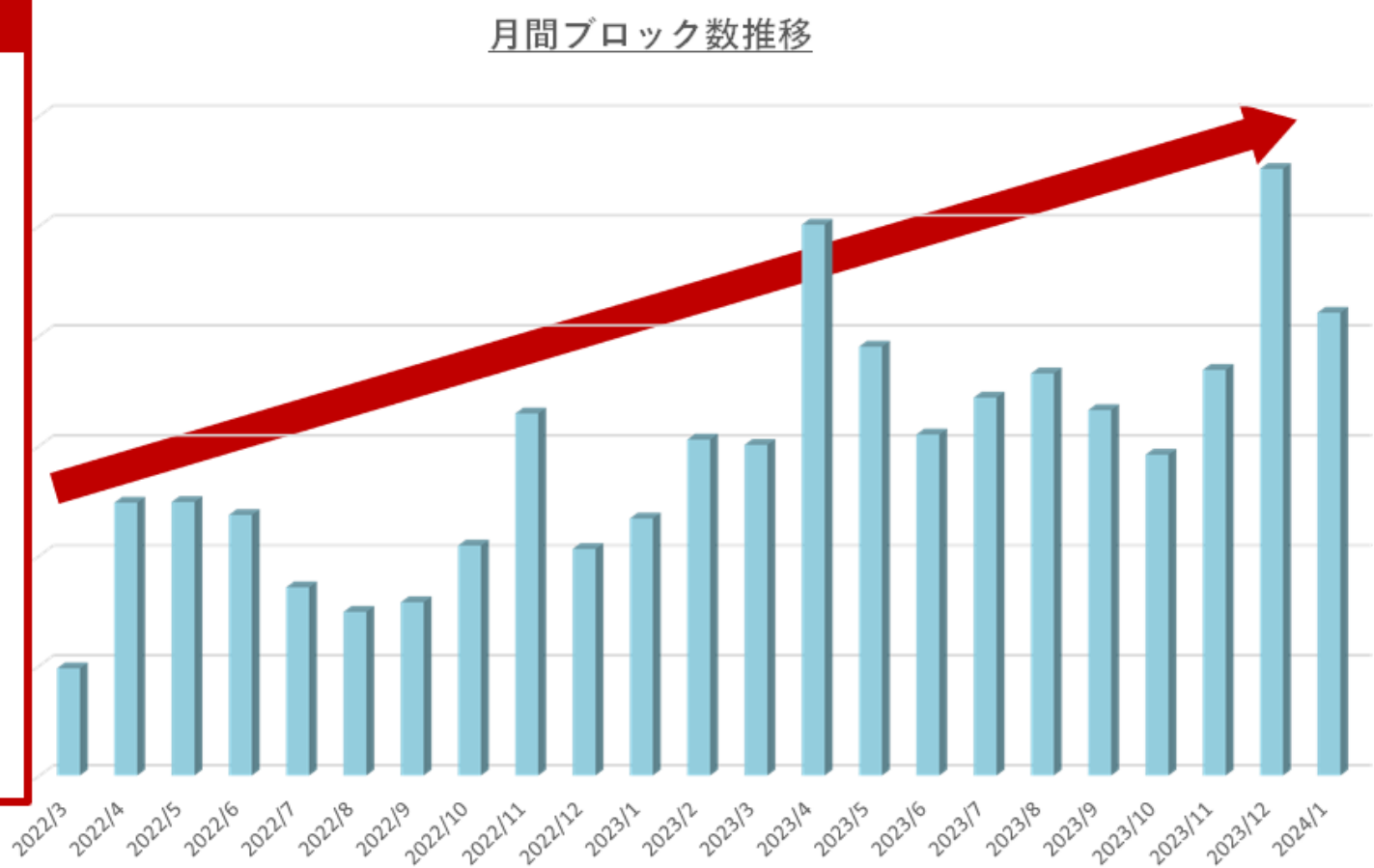
■ 危険SMS拒否設定の廃止(オプトアウト)は、Web画面にてお客様自身での設定変更が可能



危険SMS拒否設定によるフィッシングSMS検知状況

- フィッシングSMS検知による受信ブロック件数は増加傾向
- 攻撃手法の変化が激しく、受信ブロックを回避するSMS送信手法を模索していると推定

構成員限り



＋メッセージにおける「迷惑メッセージ対策機能」の提供

■ ＋メッセージアプリにて迷惑メッセージ対策機能を提供
①ブロック機能：特定ユーザからのメッセージ受信をブロック
②連絡先未登録者フィルタリング：連絡先未登録者からのメッセージ受信をブロック
③迷惑メッセージ申告：受信した迷惑メッセージ内容をドコモへ情報提供

①ブロック機能

②連絡先未登録者フィルタリング

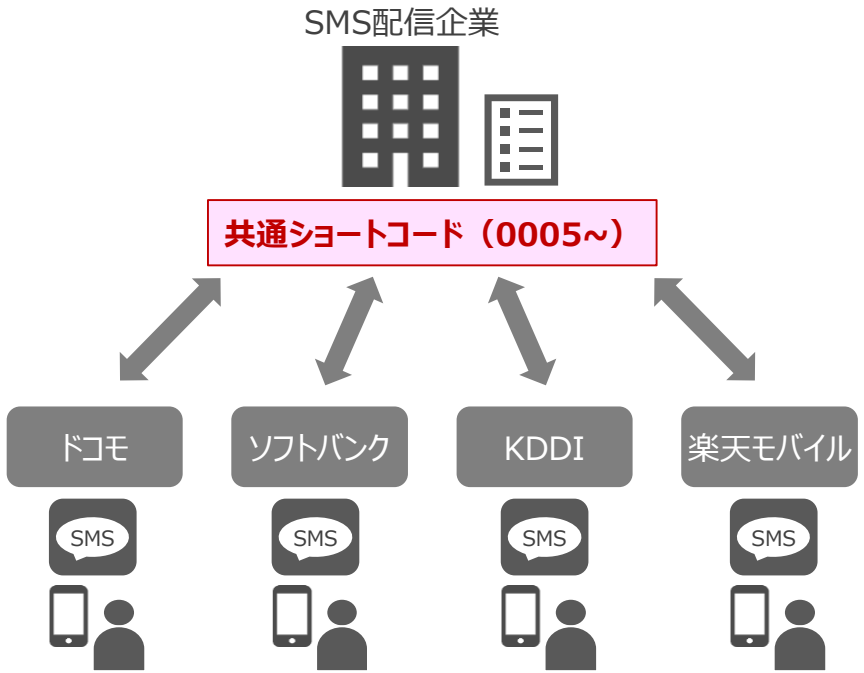
③迷惑メッセージ申告

SMS「共通ショートコード」の提供

- SMS配信企業向けに「共通ショートコード」を提供(0005から始まる8～10桁の番号を発行)
- 共通ショートコードはMNO4社の審査により発行されるため、共通ショートコードのSMSは正規メッセージと判別可能

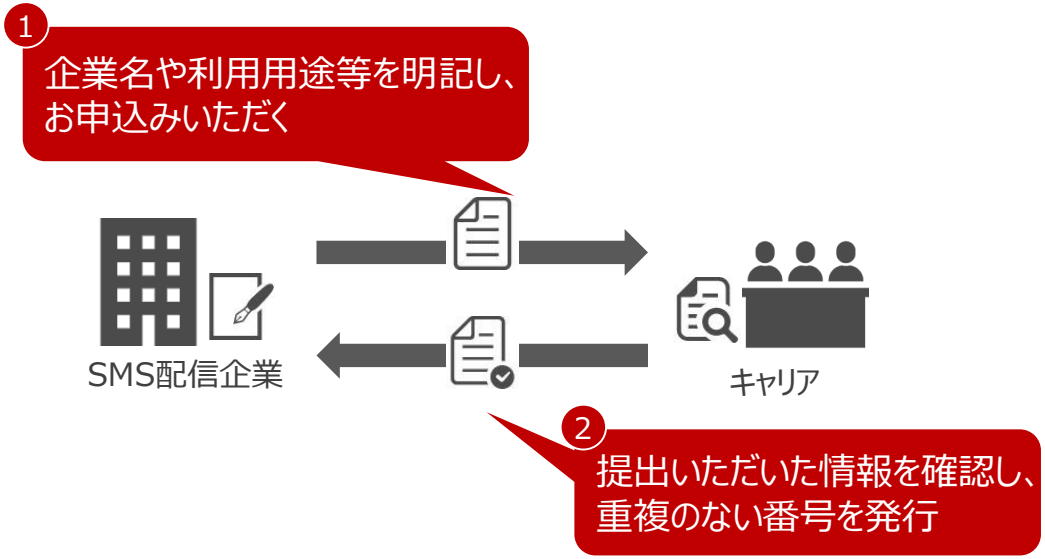
携帯キャリア間で共通の番号

MNO4社をご利用されるお客様へ1つの共通ショートコードでのSMS送受信が可能



MNO4社による審査・発行

MNO4社にて利用用途等の事前審査を実施したうえで共通ショートコードを発行

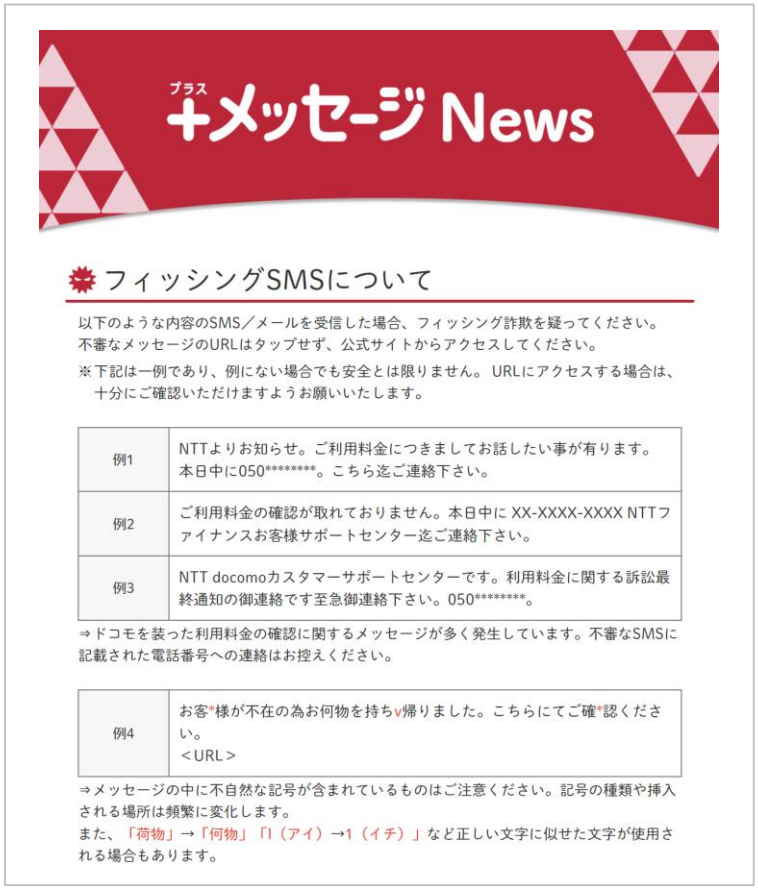


お客様への注意喚起・周知啓発の取組み

フィッシング詐欺に関する注意喚起の実施

- ドコモHPにて、フィッシング詐欺に関する事前対策や被害に遭った場合の対応方法を掲載
- フィッシング詐欺に関するSMS・+メッセージの実例を掲載し、お客様への注意喚起を実施

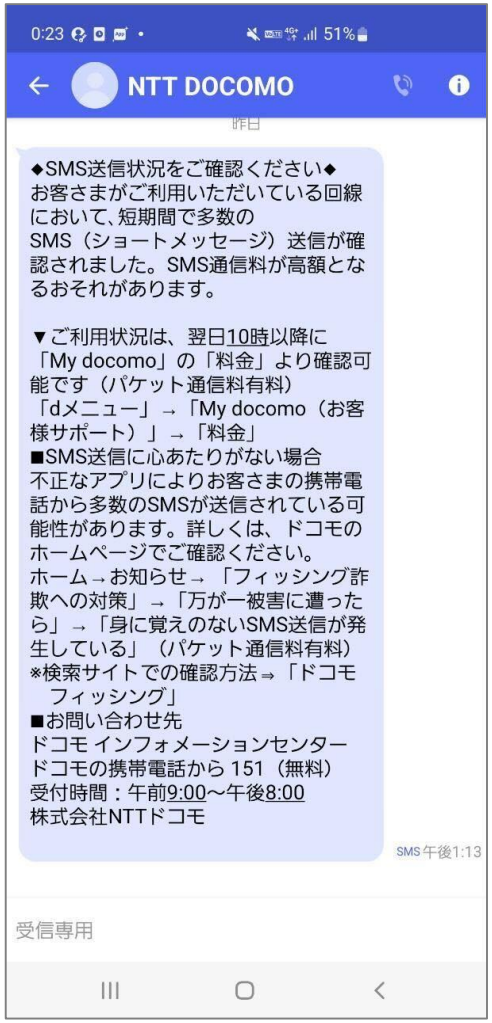
https://www.docomo.ne.jp/info/anti-phishing/



https://service.smt.docomo.ne.jp/site/mail/src/plusmessage-phishing.html

SMS送信状況に関する注意喚起の実施

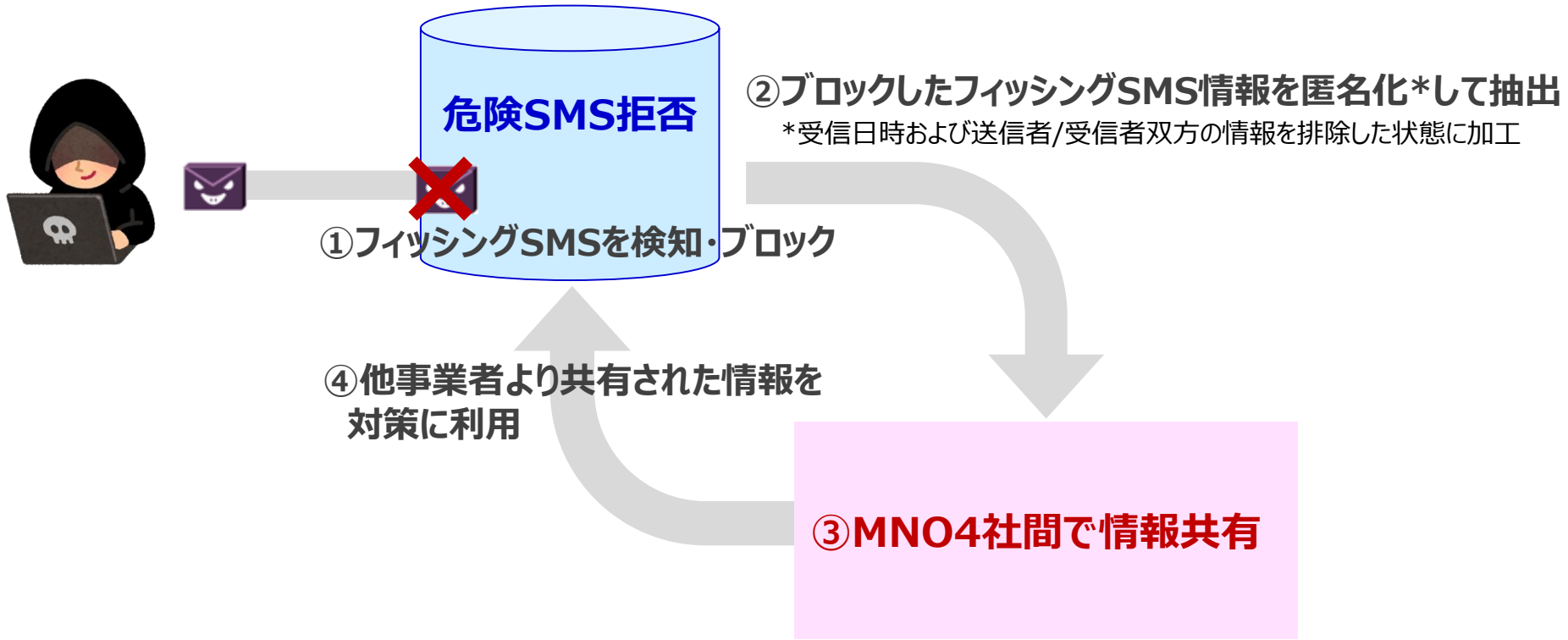
- 短期間に多数のSMS送信が確認されたお客様を対象に、2021年より注意喚起SMS配信を実施
- SMS送信状況の確認依頼、及びSMS送信に心あたりがない場合の確認方法を案内



携帯電話事業者・関係機関との情報連携

携帯電話事業者間における情報共有

- MNO4社間にてフィッシングSMS情報や攻撃手法等を情報共有(情報匿名化を実施後に共有)
- 情報共有内容を危険SMS拒否設定の検知精度向上等の対策に活用



構成員限り

関係機関との情報連携

迷惑SMS送信者への対応

- お客様申告情報等に基づき、迷惑メール・SMS送信を行う契約者に対して利用停止や契約解除等の措置を実施
- 繰り返し迷惑メール等を送信する行為の抑止を目的として、利用停止等の措置を行った契約者情報を携帯電話事業者間にて情報交換

迷惑メールを送信してくる契約者への対応状況

弊社では、お客様からお寄せいただいた情報をもとに、弊社契約約款に違反した迷惑メールが送信されたと認めた契約者に対して、契約約款にもとづき、利用停止／契約解除などの厳しい措置を講じております。
お寄せいただいた情報には間違いメールや誹謗中傷メールなども含まれておりますが、弊社契約約款に違反した迷惑メールのみを対象とさせていただいておりますので、ご注意願います。
今後も迷惑メールの根絶と快適かつ安心して、モバイル・インターネット・サービスをご利用いただける環境を整備してまいりますので、ご協力の程よろしくお願いいたします。

iモード／spモード／mopera Uを利用した迷惑メール送信者への措置

利用停止件数：NTTドコモ累計44,151回線
契約解除件数：NTTドコモ累計11,292回線
（2023年12月31日現在）

SMSを利用した迷惑メール送信者への措置

利用停止件数（SMS）：NTTドコモ累計23,500回線
契約解除件数（SMS）：NTTドコモ累計3,128回線
（2023年12月31日現在）

https://www.docomo.ne.jp/info/spam_mail/if/stop/

迷惑メール送信者の情報交換

迷惑メール送信者の情報交換

平成18年3月1日より携帯電話事業者間において、迷惑メール等送信行為により利用停止措置（契約の解除を含む。以下同じ。）を受けた加入者情報を交換しています。

1. 交換目的

一時に多数の者に対する「特定電子メールの送信の適正化等に関する法律」違反のメール送信その他の電子メール送受信上の支障を生じさせるおそれのある大量送信行為を行い利用停止措置を受けた加入者の情報を、携帯電話事業者間で交換することにより、別の事業者を渡り歩いて迷惑メール等送信行為を繰り返すことを未然に防ぐことを目的としています。

2. 対象となるお客様

平成18年3月1日以降に迷惑メール等送信行為により利用停止措置を受けたお客様を対象といたします（利用停止措置を講じた事業者において当該措置を解除した場合には対象外となります）。

また、迷惑メール等送信行為により利用停止措置を受けたお客様の契約者名、住所、生年月日等の個人情報を携帯電話事業者間において交換することは、契約約款の規定に基づいてお客様の同意をいただきます（既に契約済のお客様についても同様といたします）。

https://www.tca.or.jp/mobile/spam-mail.html

マルウェア感染による
SMS大量送信被害への特別対応

マルウェア感染によるSMS大量送信被害への特別対応

- マルウェア感染等によりお客様の身に覚えのないSMS大量送信が発生し、SMS通信料金が高額となる事例が散見
- お客様のご申告内容や事象を確認し、ドコモ受付基準に該当する場合、特別対応を実施

項目	内容
受付基準	下記①～③全てに該当する契約回線に適用 ①お客様より「不正SMS送信の請求被害に遭われた」旨のご申告をいただいていること ②ご申告月を含む含む直近３か月のいずれかの月にて、SMS通信料金が2,000円以上であること ③当社の定める問診(SMS通信料金、ご利用端末等の状況確認)、マルウェア削除の対応、再発防止措置(各種端末設定)を実施いただくこと ※受付基準を満たす場合でもドコモ判断により特別対応をお断りする場合あり
特別対応	ご申告月を含む直近３か月のSMS通信料金を減算 ※契約１回線あたり１回に限り適用

構成員限り

まとめ

まとめ

- ドコモでは「危険SMS拒否設定」をはじめとする、フィッシングSMS対策に関する機能の提供を実施しています
- ドコモHPにて、フィッシング詐欺の事前対策や被害に遭った場合の対応方法等をご紹介する他、お客様へ個別の注意喚起を実施しています
- 関係事業者間との情報連携により、フィッシングSMS対策の精度向上に向けた取組みを実施しています
- マルウェア感染等によりSMS通信料金が高額となったお客様について、ドコモ受付基準に基づき、SMS通信料金の特別対応をしています
- フィッシングSMSの攻撃手法は常に変化をしており、通信事業者の対策実施の他、お客様による対策実施やリテラシー向上が不可欠と考えます

(対策実施の一例)
- 身に覚えのない連絡先から送られてきたメール/SMSのURLをクリックしない
- 不信なサイトに個人情報を入力しない
- ID・パスワードは使いまわさず、生体認証等の認証方法を活用する